Chapitre I
Introduction à la Sécurité

Domaines de la sécurité informatique

Menaces et scénarios d'attaques

Algorithmes de chiffrement

Concepts de base liés à l'arithmétique modulaire

QUOI ET POURQUOI ?

- Quel est l'intérêt de pirater ?
  - Curiosité
  - Concurrence commerciale ou pour l'argent
  - Se montrer intelligent et se distinguer des autres
  - Ça fait plaisir de causer le mal aux autres
  - Analyser les vulnérabilités pour les corriger
- Les différents axes de la sécurité informatique
  - Protection des logiciels et droits d'auteurs
  - Protection contre les codes malveillants
  - Protection contre le spamming
  - Protection des données dans les réseaux de communication

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

LOGICIELS ET DROITS D'AUTEURS

- Comment protéger son logiciel ?
  - Protection à l'aide d'un numéro de série
  - Protection à l'aide d'un support physique
- Que veut dire pirater un logiciel ?
  - Dériver une autre version qui fonctionne sans protection
- Comment pirater un logiciel ?
  - Le meilleur moyen est d'avoir un « décompilateur » (!)
    - Exécutable ⇒ Code source en langage évolué (C++, Java, ... etc.)
  - Le désassemblage
    - Exécutable ⇒ Code source en langage assembleur

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

LOGICIELS ET DROITS D'AUTEURS

- Désassembleur
  - Permet d'afficher le programme en assembleur (WinDasm)
- Editeur hexadécimal
  - Permet de modifier le fichier exécutable (WinHex)
- Comment enlever la protection ?
  1) Lancer l'exécutable et taper un numéro de série aléatoire et retenir le message d'erreur
  2) Désassembler le fichier exécutable
  3) Chercher le texte du message d'erreur dans le programme
  4) Repérer l'instruction qui effectue un test avant d'afficher le message d'erreur
  5) Inverser la condition en utilisant l'éditeur hexadécimal

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

LES CODES MALVEILLANTS

- Programme malveillant capable d'infecter un autre en le modifiant de façon à ce qu'il puisse à son tour se reproduire
- ⇒ Virus informatique
- Programme malveillant caché dans un autre qui donne accès à la machine victime sur laquelle il est exécuté et sur laquelle il exécute des commandes à distance
- ⇒ Cheval de Troie (Trojan)
- Programme malveillant dupliqué sur plusieurs machines dont le déclenchement s'effectue à un moment déterminé pour attaquer une machine victime
- ⇒ Bombes logiques (DoS – Denial of Service)
- Programme malveillant qui collecte des informations de la machine sur laquelle il est exécuté
- ⇒ Espiogiciels (Spaywares)

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

LE SPAMMING

PUB

L'objectif ce n'est pas d'attaquer

Surcharger le serveur

ARNAQUE

On propose une offre

Confiance

On demande de l'argent

HOAX

Le message est diffusé par les utilisateurs eux-mêmes

Sensibiliser les utilisateurs afin qu'ils diffusent le message

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

LES HOAX

Je vous envoie ce truc parce que c'est trop surprenant, mon vœu s'est réalisé !! J'espère que ça te fera plaisir : 20min après avoir fait ça, mon vœu s'est produit. La personne qui me l'a envoyé m'a dit que son vœu avait fonctionné 15 min après avoir lu le message. Le hasard n'existe pas ! Essaie-le pour voir ! Fais un vœu avant que le comptage ne soit fini !! Commence à descendre après avoir formé ton vœu : 10 … 9 … 8… 7 … 6 … 5 … 4 … 3 … 2 … 1. Fais un vœu ! Envoie cet email à 10 personnes avant une heure. Si tu fais, ton vœu se réalisera. Si tu ne le fais pas, le contraire de ton vœu va se produire! Bonne chance. Condition d'utilisation le renvoyer au plus grand nombre de personnes. Recopies le message et colle-le dans un nouveau : Al Qayum, Al Majid, Al Wajid, Al Wahid, Al Ahad, Al Samad, Al Quadir, Al Malik, Al Rahman, Al Rahim. Allah n' échoue jamais. Envoyez ce message à neuf personnes, vous obtiendrez de bonnes nouvelles demain. Si vous le négligez, mauvaise chance pendant neuf années. C'est vérité prouvée. Ne prenez pas le risque. Seulement envoyer à neuf messages au nom d'Allah

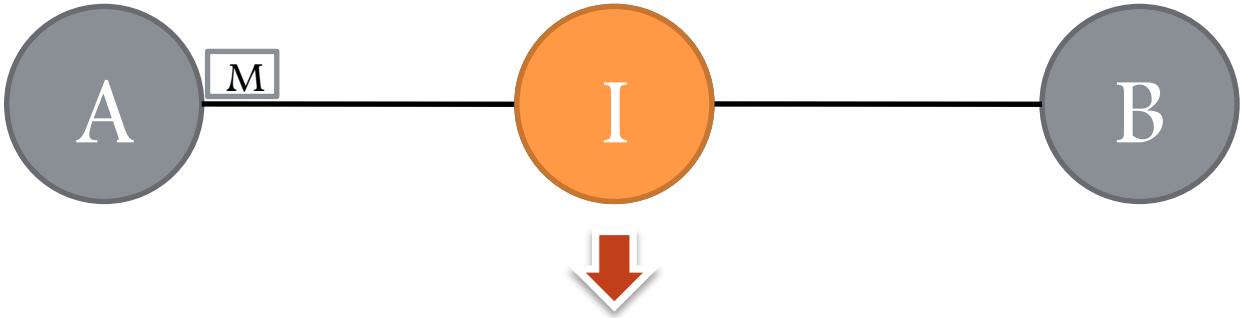
Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

LES ARNAQUES

Excusez-moi pour cette intrusion, je suis CORINNE BURIERE d'origine française et cela fait deux 2 jours que J'ai contacté une association qui s'occupe des enfants démunis et pas de réponse. Mais j'ai pu me mettre en contact avec vous ceci grâce à la volonté de DIEU. Cela fait quelques mois que j'ai été atteint d'un cancer en phase terminale détectée trop tard et selon les dires de mon médecin, je n'ai plus assez de temps à vivre. En ce moment je suis hospitalisée dans un hôpital à Londres. J'ai toujours privilégié le service de ma nation au détriment de ma propre santé et voilà aujourd'hui cela me rattrape, mais je suis fière d'avoir pu aider des gens autour de moi et je pense pouvoir continuer à le faire à travers vous. J'ai Perdu mon mari et mes deux enfants dans un crash d'avion qui s'était produit à New York. J'aimerais que vous soyez le bénéficiaire de toute ma fortune qui est d'une somme exactement chiffrée à 1.500.000 euros que vous utiliserai pour aider les enfants pauvres et déshérités vu que mes jours sont comptés. Aussi, ce matin j'ai reçu un message de ma banque me disant que l'État aimerait récupérer mes fonds après ma mort vu que je n'ai pas d'héritier(e). Veuillez m'aider en acceptant mon offre. Répondez-moi vite. Que le Seigneur vous garde.

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

PROTECTION DES DONNÉES DANS LES RÉSEAUX DE COMMUNICATION

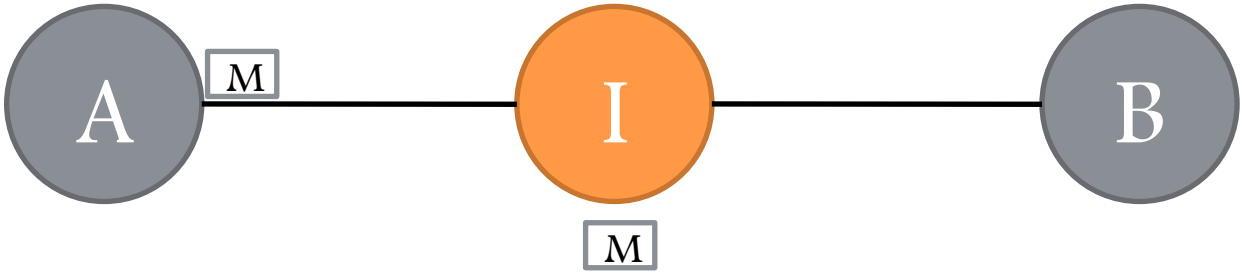


- Routeur dans un réseau filaire
- Point d'accès dans un réseau mobile
- Machine intermédiaire dans un réseau mobile ad hoc

Attaquant Potentiel

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

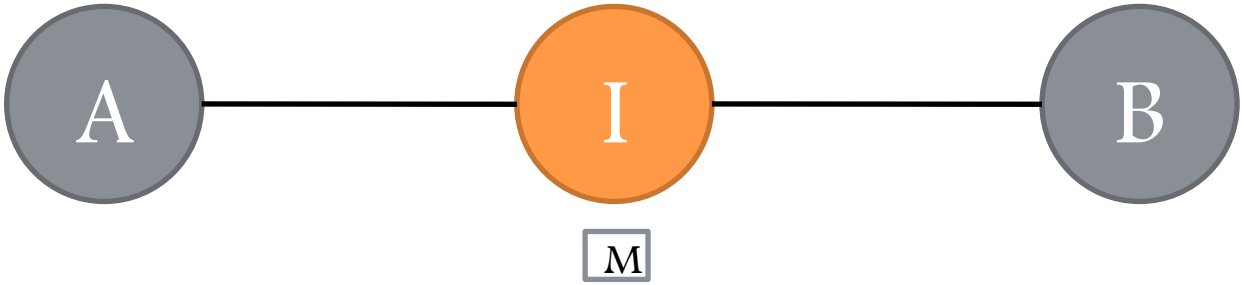
L'INTERCEPTION



La confidentialité

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

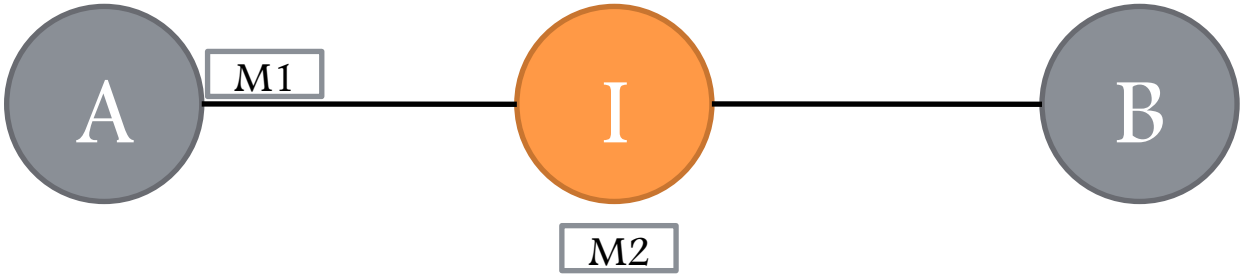
LA FABRICATION



L'authentification

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

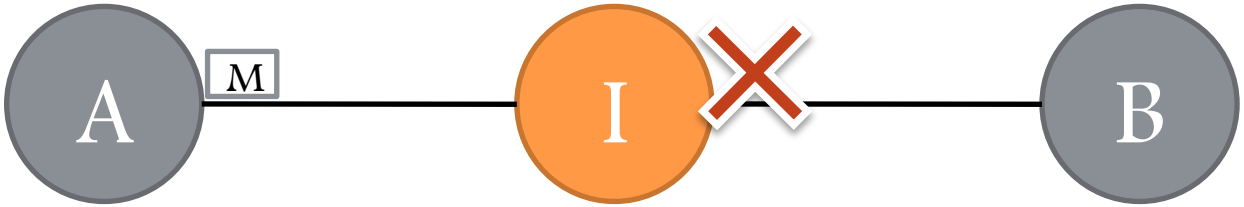
La modification



L'intégrité

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

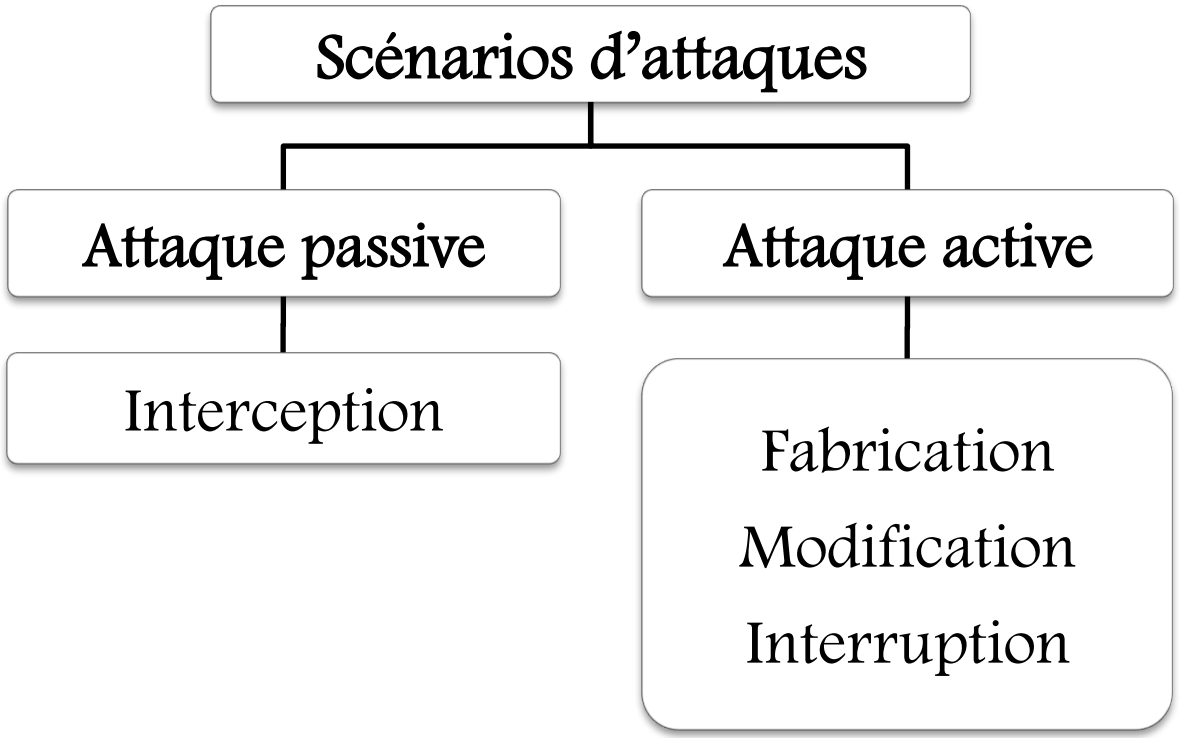
L'INTERRUPTION



Disponibilité

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

Les scénarios d'attaques



Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

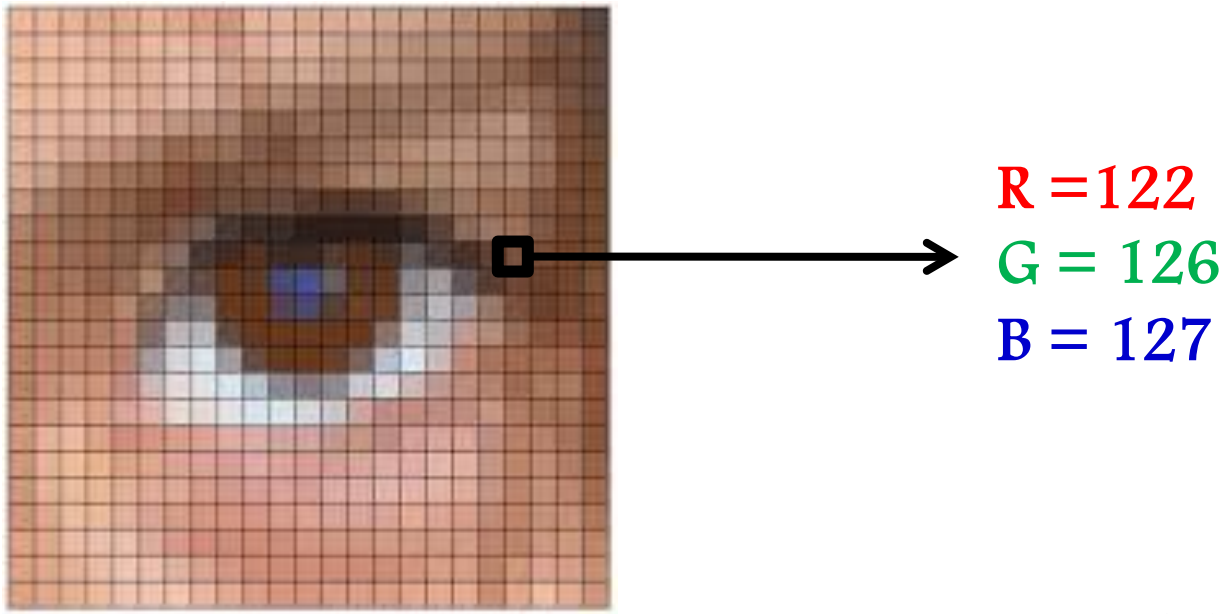
La stéganographie

- Dissimuler un secret dans un support anodin
- Stéganographie classique
  - Dissimuler un message secret dans un autre message
  - Exemple : Collecter les mots de positions impaires
    - Il ne faut pas tuer Jules César car il n'est pas le vrai coupable
    - Il ne faut pas tuer Jules César car il n'est pas le vrai coupable
    - Il faut tuer César il est le coupable
- Stéganographie moderne
  - Les trames ⇒ Exploiter les champs non-utilisés
  - Les exécutables ⇒ Déclaration des variables strings inutiles
  - Images ⇒ Exploiter les bits de poids faibles du pixel

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

LA STÉGANOGRAPHIE MODERNE

- Chaque pixel d'une image (format bmp) est représenté par 3 nombres codés sur 8 bits
  - R ⇒ l'intensité du rouge
  - G ⇒ l'intensité du vert
  - B ⇒ l'intensité du bleu



Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

LA STÉGANOGRAPHIE MODERNE

- Image composée de deux pixels
  - R_1 = 01001110 G_1 = 01101111 B_1 = 11111111
  - R_2 = 01110011 G_2 = 01110110 B_2 = 10101010
  - M = 101100011011
  - R_1 = 01001110 G_1 = 01101111 B_1 = 11111100
  - R_2 = 01110001 G_2 = 01110110 B_2 = 10101011
- Très discret
- Permet de cacher des messages de tailles importantes
  - Image 40×40 ⇒ 40×40×6 = 9600 bits ⇒ 1200 caractères
- Il faut transmettre les fichiers en format bmp
- Toute compression fait perdre le message caché

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

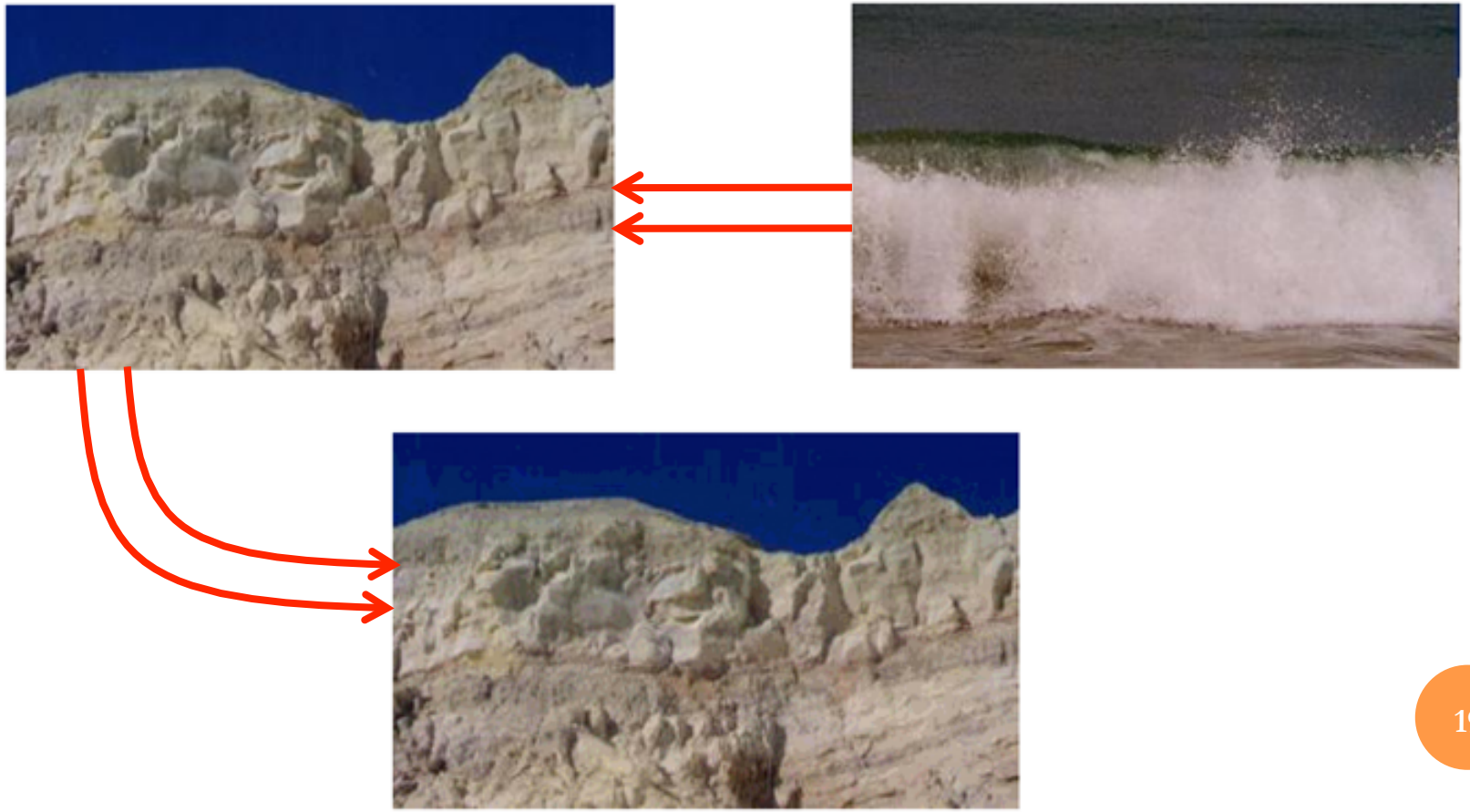
La stéganographie moderne

- Exemple 1 : Message caché dans une image

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

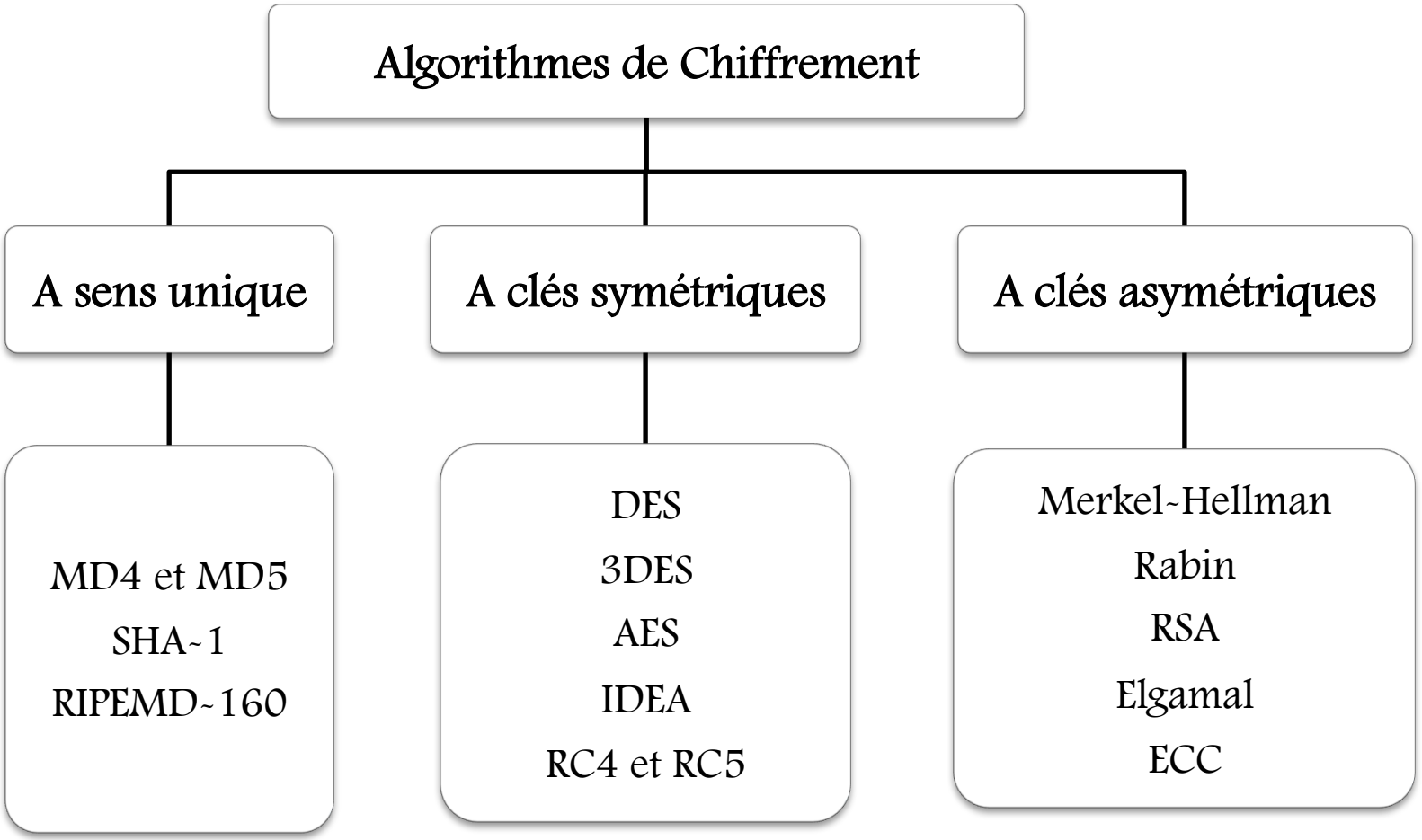
La stéganographie moderne

- Exemple 2 : Image cachée dans une image



Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT MODERNE



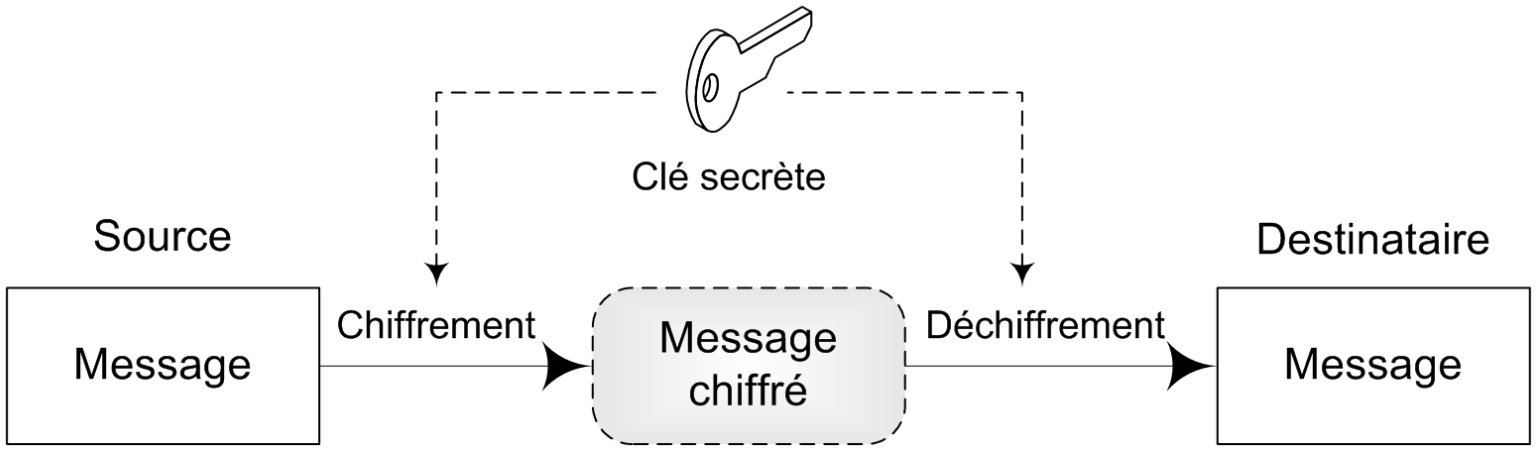
Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT À SENS UNIQUE

- h=H(M)
- La valeur de h est de longueur fixe et inférieure à M
- A partir de h, il est impossible de retrouver M
- Il est difficile de trouver M' tel que H(M')=h

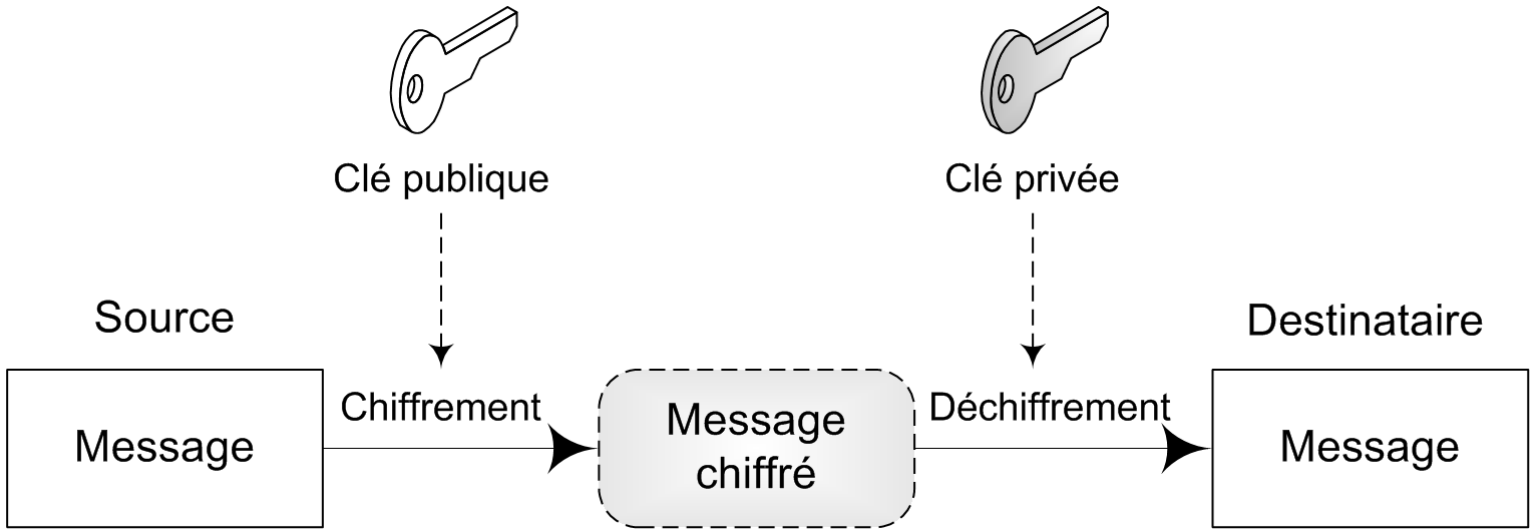
Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT À CLÉS SYMÉTRIQUES



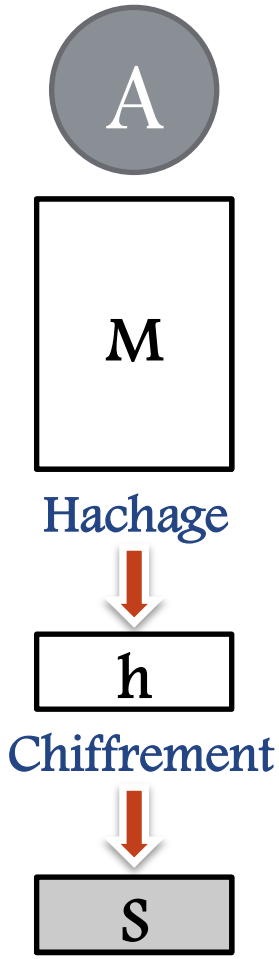
Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

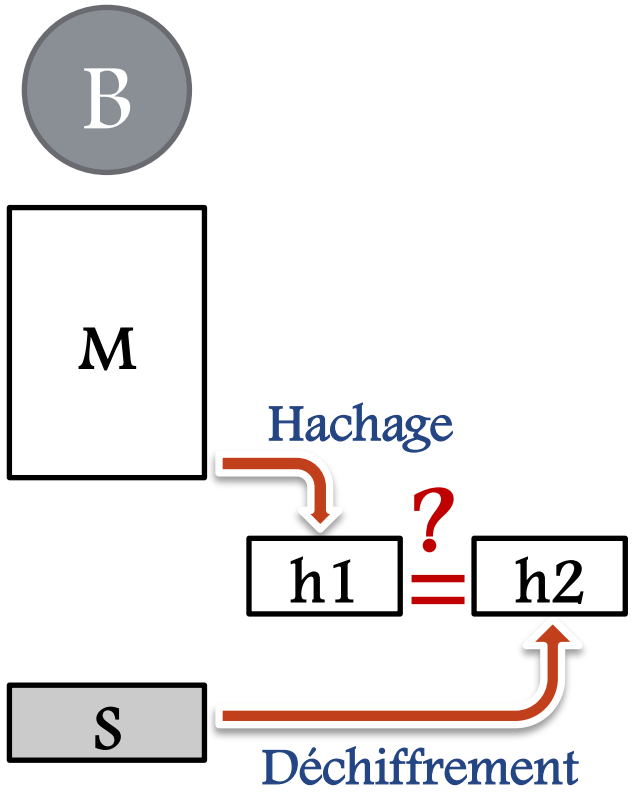
CHIFFREMENT À CLÉS ASYMÉTRIQUES



Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

SIGNATURE NUMÉRIQUE

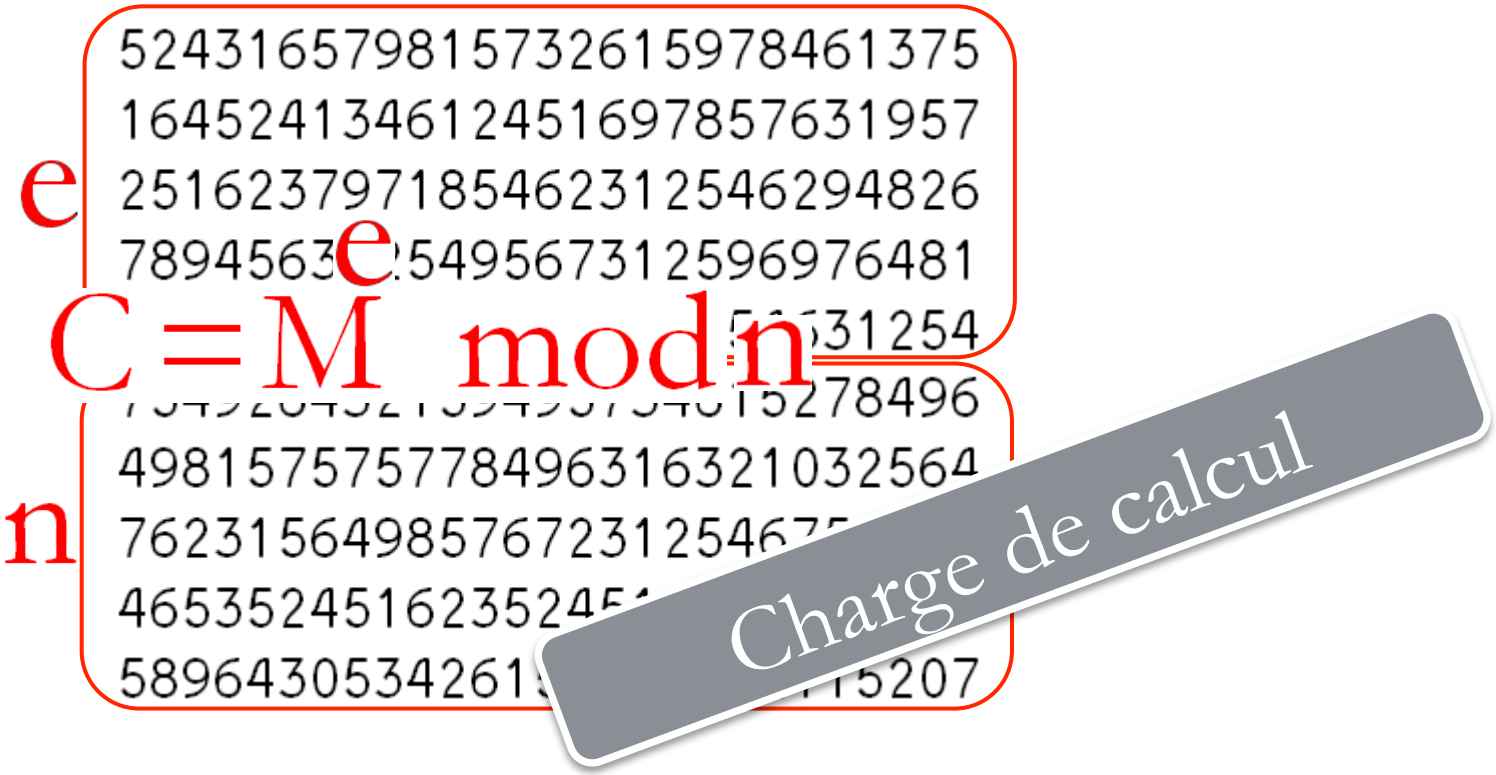




Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

SYMÉTRIQUE OU ASYMÉTRIQUE ?

- Une clé publique RSA de 512 bits :



Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

SYMÉTRIQUE OU ASYMÉTRIQUE ?

- Soit une clé publique RSA de 512 bits, tel que n =

```
1094173864157052742180970732204035761200373294544920599091384
2131476349984288934784717997257891267332497625752899781833797
0765372440271467435315933543338973
1026395928297411057720541965739916759007165678080380668033419
33521790711307779
x 1066034883801684548209272203600128786792079585759892915222706
08237193062808643
```

Factorisation d'un entier à 155 chiffres.

- Institut National de Recherche en Mathématiques et en Science Informatique d'Amsterdam
  - 300 ordinateurs durant 105 jours de calcul !!

Robustesse

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

ALGORITHME D'EXPONENTIATION RAPIDE

- $C = B^A \bmod N$
- A partir du triplet (P, J, R) / P=B, J=A, et R=1
- Si J est pair $\Rightarrow$ ($P^2 \bmod N$, J/2, R mod N)
- Si J est impair $\Rightarrow$ ($P^2 \bmod N$, (J-1)/2, R×P mod N)
- Si J=1 $\Rightarrow$ C=R×P mod N

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

ALGORITHME D'EXPONENTIATION RAPIDE

- **$C = 150^{233} \bmod 437$**
- A partir de (P=150, J=233, R=1)

→ $(150^2 \bmod 437, (233-1)/2, 1\times150 \bmod 437) = (213, 116, 150)$

→ $(213^2 \bmod 437, 116/2, 150 \bmod 437) = (358, 58, 150)$

→ $(358^2 \bmod 437, 58/2, 150 \bmod 437) = (123, 29, 150)$

→ $(123^2 \bmod 437, (29-1)/2, 150\times123 \bmod 437) = (271, 14, 96)$

→ $(271^2 \bmod 437, 14/2, 96 \bmod 437) = (25, 7, 96)$

→ $(25^2 \bmod 437, (7-1)/2, 96\times25 \bmod 437) = (188, 3, 215)$

→ $(188^2 \bmod 437, (3-1)/2, 215\times188 \bmod 437) = (384, 1, 216)$

→ **$C=384\times216 \bmod 437=351$**

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

ALGORITHME D'EXPONENTIATION RAPIDE

- $C = 150^{233} \bmod 437$
- $233 = 11101001_{(2)}$

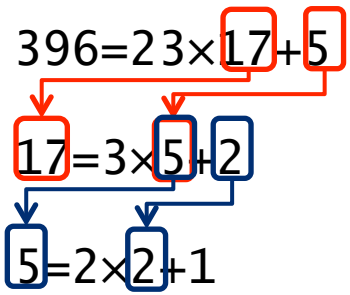
1	150
0	$150^2 \bmod 437 = 213$
0	$213^2 \bmod 437 = 358$
1	$358^2 \bmod 437 = 123$
0	$123^2 \bmod 437 = 271$
1	$271^2 \bmod 437 = 25$
1	$25^2 \bmod 437 = 188$
1	$188^2 \bmod 437 = 384$

$150 \times 123 \times 25 \times 188 \times 384 \bmod 437 = 351$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

ALGORITHME D'EUCLIDE ETENDU (LES ÉQUATIONS DIOPHANTIENNES)

- $396X+17Y=1$
- $396=23\times17+5$

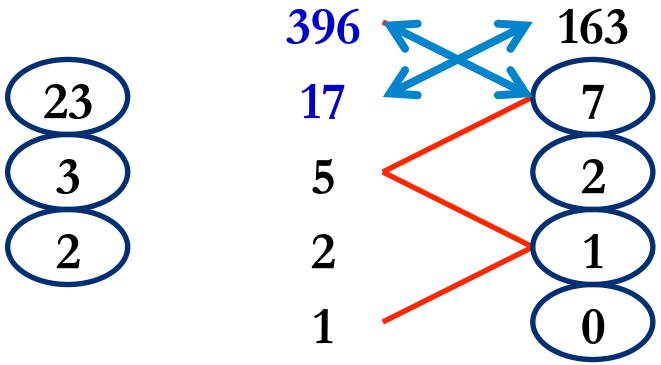


- $1 = 5-2\times2$
  $= 5-2\times(17-3\times5)$
  $= 5-2\times17+6\times5$
  $= 7\times5-2\times17$
  $= 7\times(396-23\times17)-2\times17$
  $= 7\times396-161\times17-2\times17$
  $= 7\times396-163\times17$
  $= 396\times7+17\times(-163)$ ⇨ $\{X=7, Y=-163\}$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

ALGORITHME D'EUCLIDE ETENDU (LES ÉQUATIONS DIOPHANTIENNES)

$396X+17Y=1$



$396 \times 7 - 17 \times 163 = 1$ ⇨ $\{X=7, Y=-163\}$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia